1 引言

1.1 全民战“疫”，远程办公需求爆发

新春过后，受新型冠状病毒疫情影响，“少出门、不聚集”已成为社会共识，企事业单位为抗击突发疫情、切实保障员工健康，纷纷选择让员工留在家中远程办公，以医院、疾控为代表的部分单位为降低病毒感染风险，甚至要求其合作伙伴能够以远程接入的方式提供技术支持。

远程办公概念已普及多年，且部分企事业单位已部署了支撑远程办公的系统。但在过往，远程办公仅定位服务于少部分出差、驻外、SOHO 的远程用户接入使用，而着眼当下，在全社会积极生产抗击疫情的热潮中，为了确保“停工不停产”，远程办公已成为多数企事业单位开展生产业务的主流办公形式，远程办公的接入用户规模大幅提升，接入后需访问的应用类型大幅增加，业务交互和操作也更为复杂，这给远程办公技术的运用提出了更为严苛的要求。

1.2 远程办公的场景简析

企事业单位开展远程办公，主要需实现的效果是员工在办公场所之外的地方，使用企业配发的 PC、个人 PC、智能移动终端等设备，以虚拟隧道的方式通过互联网安全访问企业内部的信息化系统和应用资源，实现办公业务的交互。

典型的远程办公操作包括应用系统远程访问、文件资料共享、信息共享交互、信息系统远程运维等。例如，员工远程访问 OA、ERP、CRM 等业务系统并提交业务操作，使用企业私有的即时通信系统、邮件系统、视频会议系统进行信息交互，远程运维企业内部的 IT 资产等。

当前，主流的远程办公技术实现，由其接入的终端类型及方式差异，大体可分为以下几类：

- PC 远程接入：指远程用户使用 PC，通过 SSL VPN 与企业内网建立安全隧道实现接入，一旦完成接入，其访问应用系统的操作体验则基本近似于办公场所内 PC 的访问体验；
- 虚拟桌面云：指远程用户通过桌面云瘦客户机或在 PC 上运行软件形态的 APP，以安全隧道的方式（多由 SSL VPN 接入系统提供）接入企业自建的虚拟桌面云系统，其原理相当于企业在内网为远程用户创建了专用的虚拟 PC，远程用户安全接入系统并远程控制该虚拟 PC 完成业务交互；
- 移动终端远程接入：随着 BYOD 运用的普及，越来越多的企业应用开始提供针对移动端的访问接口，远程办公用户可利用个人移动终端，以安全方式远程接入企业内网，并以 APP 等形式访问企业应用系统实现业务交互。

1.3 远程办公，信息安全迎来“大考”

相比在企业办公场所本地办公，远程办公尽管提供了更为灵活、便捷的业务开展形式，但由于其使用企业网络外部的终端系统、利用开放的互联网资源、且其“远程接入”的特点本身就给管理者带来了天然的挑战，因此安全问题首当其冲的成为了当前企事业单位采用远程办公时需考虑的核心问题，鉴于突发的疫情使远程办公的运用程度激增，其安全性也将迎来一场“大考”。

企事业单位在开展远程办公的同时，涉及身份认证、安全接入、访问交互等多个环节，可能对其系统造成安全危害的风险则包括多个方面。

在当前全国人民抗击疫情的关键时期，为保障广大企事业单位的生产业务安全，企事业单位 IT 管理者则更应关注信息系统的安全性，尤其是采用适当的方案消减远程办公带来的诸多风险，确保安全远程办公开展。

2 安全远程办公需求分析

2.1 远程办公安全风险分析

基于以上对远程办公技术实现及场景的分析，远程用户无论采用 PC 终端、桌面云系统或智能移动终端接入企业网络，其过程均可概括为“远程办公用户经过认证，通过其终端系统，并利用网络搭建隧道，实现企业内网接入”。

因此，远程办公的安全风险主要包括以下：

- **身份冒用风险：**攻击者可通过社工、口令破解等手段，盗用远程办公用户的登录 ID 及口令，并仿冒合法用户接入企业网络；
- **带病接入风险：**远程办公用户使用的 PC 或移动终端本身已遭到入侵或具有明显漏洞，此类终端一旦接入企业内网，则极有可能被攻击者利用对企业网络造成安全危害；
- **数据泄密风险：**远程办公用户基于开放互联网访问应用系统，由于加密算法强度、密钥失窃等问题，可能造成加密的业务数据被攻击者破解，从而造成数据泄密；
- **越权访问风险：**远程办公用户规模较大、角色较多，管理者在进行接入用户的授权管理过程中难于实现精细化、细粒度，则容易造成接入用户授权过度，导致越权访问；
- **恶意行为风险：**远程办公用户接入企业内网后，可能开展恶意攻击活动或非故意的误操作，而由于其“远程”、“加密”的特点，相对本地办公用户则更加难于审计和追溯。

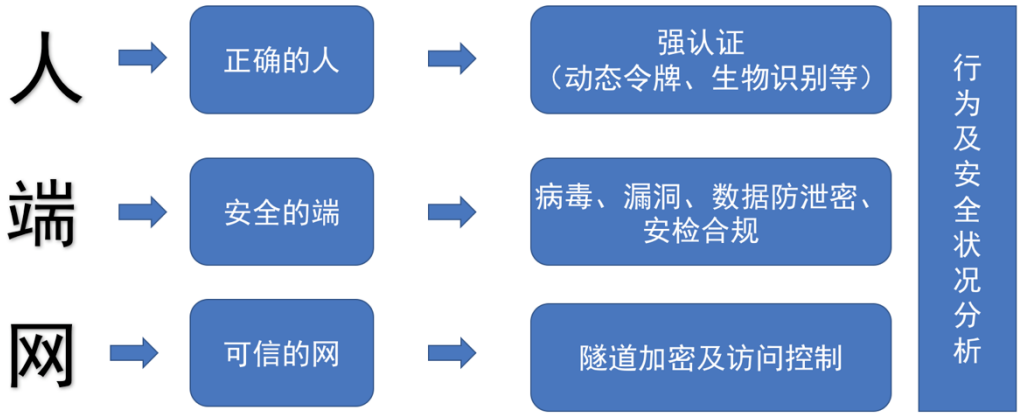
值得强调的是，由于使用智能移动终端接入企业网络实现远程办公的场景已日益普遍，因移动终端自身特有的脆弱性而引发的信息泄密风险则更应引起高度关注，具体包括：

- **终端丢失风险：使用智能**移动终端进行远程办公，势必造成企业业务数据在移动终端上落地存储，手机、PAD 等 BYOD 设备一旦失窃，则其保存的企业业务数据、用户认证信息等则将被泄漏；
- **恶意 APP 风险：智能移动终端可以自由安装海量的 APP，由于缺乏统一的检测和管理，手机、PAD 等设备极易安装被植入间谍软件功能的软件，危害企业业务数据安全；**
- **隧道滥用风险：智能移动终端同时安装个人生活应用及企业生产应用，而一旦系统级的 VPN 隧道建立，则个人生活应用在特定情况下也可通过 VPN 隧道接入企业内网，给企业业务数据安全造成威胁；**
- **主动泄密风险：由于智能移动终端操作简便，并具有多网络接入功能，可通过**截图、复制等方式轻易的拷贝企业业务数据并通过其他网络转发造成信息泄密。

2.2 安全需求分析

远程办公安全的核心三要素可归结为“人”、“端”和“网”。“人”指要开展远程办公的具体用户；“端”则指远程办公用户接入企业网络使用的终端系统；而“网”则指远程用户接入企业网络所建立的网络隧道。

确保安全远程办公的开展，实际可概括为**“确保正确的人，使用安全的端，通过可信的网”**访问企业业务系统，实现办公业务交互。



2.2.1 正确的人——确保远程用户身份合法

确保远程办公接入者是“正确的人”，需对远程接入用户执行严格的身份认证，确保用远程接入用户的凭证合法。

2.2.1.1 多因素认证需求

鉴于单独的口令认证容易产生弱口令、口令暴露等风险，应采用多因素认证方式，要求远程办公用户必须通过两种或以上认证机制后，方可允许接入。

考虑远程办公用户的接入体验，多因素认证可考虑口令认证与其他认证手段相结合的方式，为了不额外增加远程办公人员的口令记忆难度，口令认证应能够与企业现有的认证系统实现联动。

2.2.1.2 采用动态认证方式

出于提升认证强度的考虑，多因素认证应在传统静态口令的基础之上，运用动态认证的方式，进一步提升认证强度，例如通过生物识别、设备指纹技术等。

同时，采用动态认证方案应充分考虑其运用成本及适用场景因素，应尽可能在不增加硬件令牌、Ukey 的情况下实现，避免高昂的投入、复杂的使用方法给企

业带来过度的负担，保证远程办公的便捷性与易用性。

2.2.2 安全的端——确保接入终端环境安全

确保远程接入用户使用“安全的端”，主要是在允许用户接入之前，对终端进行全面的主机健康检查及安全配置检查，确保接入终端不存在漏洞，且采用了符合企业合规要求的安全配置。由于接入终端类型不同，终端安全需求需区分 PC 终端及智能移动终端。

2.2.2.1 PC 终端安全

针对远程接入的 PC 终端，需要基于单位的规章要求进行合规检查，规范终端入网流程，保障入网终端的安全可信；同时对于接入的终端的安全状态进行反复评估，保证入网终端的安全基线是标准的、可控制的，可修复的；还要具备实时的终端安全防病毒功能、漏洞风险发现和修复能力，即使在不连接内网管理平台情况下，也能够通过互联网进行特征库和漏洞的防护及修复。

云桌面在远程办公中同样也有一定占比，虽然数据不落在远程办公终端上，但通过网络、应用数据流转同样有病毒威胁及漏洞利用的可能，同时管理中安全策略不完善，也容易导致安全的风险。

2.2.2.2 移动终端安全

针对远程接入的移动终端，也需要构建一套移动终端的安全防护以及合规入网检查体系，来保障移动终端免受病毒木马侵扰，避免移动终端被攻击者利用成为渗透企业内网的跳板。并可以根据移动终端杀毒扫描结果、终端是否 root/越狱等结果来匹配不同的授权策略。

需要构建一套设备环境安全系统，确保用户在工作过程中设备所处环境是否存在安全风险，可提前感知，提前预防，做到有安全风险可提前预防。同时确保在当前复杂的互联网环境下移动办公终端设备的安全性，保证移动终端在发生被病毒、木马恶意入侵的情况下，单位内部办公数据不被盗取。

需要建立一套单位内部专属的应用管理平台，确保应用的全生命周期的安全性，从应用的上架、更新、管理、下架等过程，确保移动应用的架构和使用安全。

针对分散的移动终端设备，需要建立一套安全、高效的统一管理平台，将设备的全生命周期安全、高效的管理起来，确保参与单位内部移动办公的设备，管理方便、安全风险随时可见。

需要建立业务安全体系，确保移动终端中个人数据与企业内部数据隔离存储，互不影响，保证单位内部办公数据不被泄漏。确保用户在登录过程中用户身份的真实性和可靠性，确保用户信息不被仿冒。保证有权限的用户才可访问相应的内部业务系统。

需要构建一套数据安全保护系统，确保移动终端中的办公数据安全存储在移动终端，需实现加密存储，即使数据丢失，被其他人拿到数据后依然无法阅读。

还需保证数据在使用过程中不被截屏或拍照外发。

2.2.3 可信的网——确保访问权限精细控制

2.2.3.1 采用高强度加密算法

由于虚拟专网（VPN）由 Internet 承载，远程办公用户通过 VPN 访问企业内部的业务系统，实际上是由互联网进行传输的，为了保证企业业务安全，尤其是业务数据的私密性和完整性，远程接入 VPN 技术必须使用较高强度的加密算法。此外，鉴于《密码法》、等级保护制度等的要求，相当一部分客户在运用加密技术时，必须采用我国专有的商用密码算法。

2.2.3.2 实施精细化、细粒度访问控制

对企业 IT 运维人员而言，解决企业各类人员、各类应用、各类系统、各类角色权限之间的安全问题和易用性，是摆在 IT 运维人员面前的一大难题。如果不建立一个完整的用户授权机制，那么一个“非法用户”就能轻易访问到所有业务系统或者是业务系统中的所有功能。因此业务系统都需要有一个或多个权限系统来实现访问权限检测，让经过授权的用户可以正常合法的使用已授权功能，而对那些未经授权的“非法用户”将会将他们彻底的“拒之门外”。避免发生用户越权使用业务系统造成的越权后果，同时，对于系统安全来讲减少外部攻击的攻击面。

2.2.3.3 远程访问行为可审计、可追溯

具备安全措施的同时，还需要远程接入办公系统具备全面的访问日志审计以及异常行为建模分析能力。做到所有远程办公终端进入单位内网期间的业务系统登录、访问情况，以及单位文件和核心资产数据使用情况都可定位、可记录。同时最好具备桌面水印能力，对于窃取数据行为进行震慑和发现，且能全程审计可查。

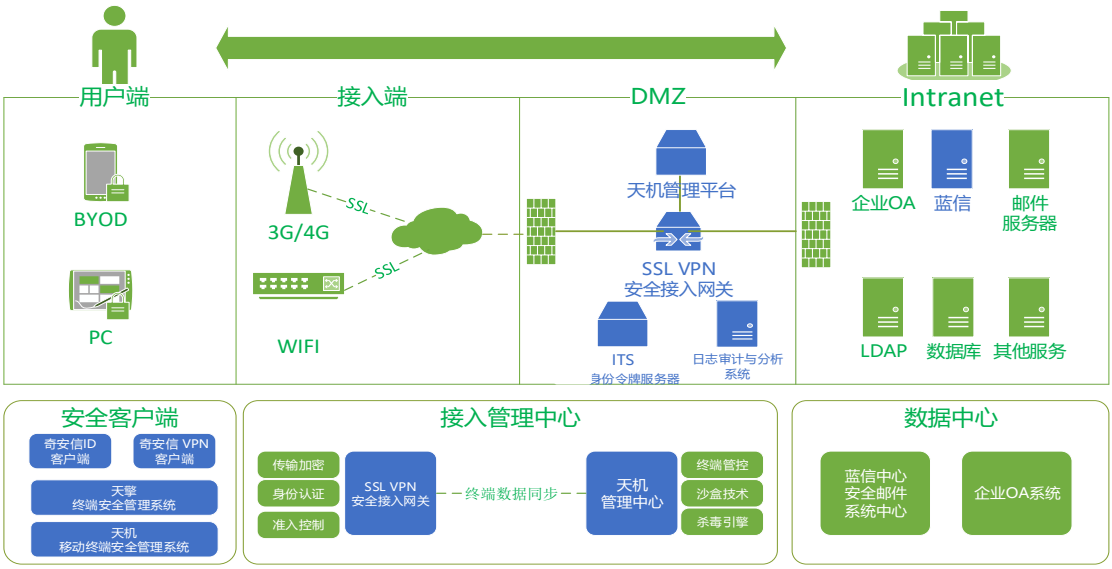
3 奇安信安全远程办公解决方案

奇安信集团历经实战，针对信息基础设施安全刚需，推出了安全远程办公解决方案。

3.1 总体方案设计

基于以上对远程办公场景、安全风险及需求分析，对应“正确的人”、“安全的端”及“可信的网”3 大安全需求，本方案通过建设远程用户多因素认证子系统、终端检查及合规检测子系统及安全接入及访问控制子系统，确保安全远程办公开展。

同时，考虑智能移动终端因其自身脆弱性，在远程办公过程中将引入其他风险，通过移动办公安全加固子系统设计针对移动终端远程办公场景实现进阶安全防护。



如上图所示，本方案通过 8 款产品无缝配合，针对远程办公过程中的身份安全、传输安全、权限控制、终端安全、行为审计 5 方面提供安全保障方案。同时，从终端安全、线路安全、应用安全、平台安全、数据安全、业务安全对智能移动终端远程办公场景提供安全加固。

3.2 远程用户多因素认证子系统

该子系统运用多因素认证、动态认证方式，对远程接入用户执行严格的身份认证，确保远程接入用户身份安全。同时，还通过单点登录设置，降低用户记忆口令、频繁登录带来的用户体验影响。

3.2.1 多因素认证设计

本方案通过奇安信身份安全认证系统（奇安信 ID）+奇安信 SSL VPN 安全接

入网关系统的有机结合，采用多因素认证及生物识别及设备指纹的技术，实现了共 18 种认证方式，包括账号密码、证书认证、LDAP 认证、AD 认证、Radius 认证、POP3 认证、SMTP 认证、IMAP 认证、HTTP 认证、数据库认证、OCSP 认证、天鉴 ID 认证、二维码认证、短信验证码认证、Radius 动态口令、邮箱验证码、蓝信认证和多因素认证。

并且可以将其中任意 4 种方式组合启用，并且配合硬件特征码绑定策略组合使用，满足客户特定应用场景的强身份认证需求。具体包括：支持本地用户名/密码认证提供基本的身份认证方式，可利用此方式为基石与其他认证方式结合。支持数字证书认证并提供安全接入平台系统设备自建 CA 中心功能提供自建 CA，可极大的降低企业使用成本并可与第三方 CA 体系进行结合。与第三方认证体系的无缝集成可与 LDAP，Microsoft AD，RADIUS 等第三方认证体系进行无缝集成，便于接入人员身份的统一管理。多样化的身份认证方式以及组合认证方式，保障了企业用户账号的安全性。

3.2.2 单点登录设计

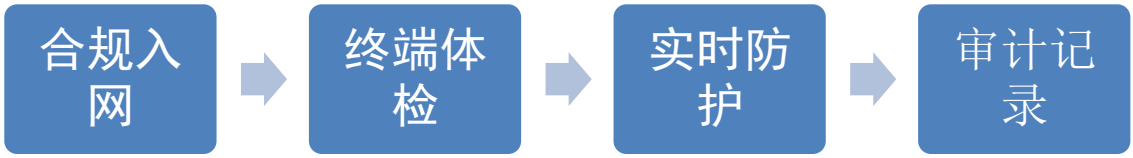
为兼顾使用体验和安全性，本方案可实现最小授权应用门户和多业务系统单点登录。奇安信身份令牌服务平台授权机制以多个安全策略纬度为中心。用户登录时，会根据用户的属性查询用户的相关安全策略的分配情况，以决定授予用户哪些服务资源，对用户的哪些服务访问采取单点登录策略，对用户的主机绑定策略，以及对用户执行哪些安全策略检查。多纬度的授权机制保证了各个安全策略能够独立制定，并分别应用在不同用户身上。在移动办公系统逐渐增多、各个系统间用户名/密码不同的情况下,为用户提供企业应用一键单点登录的功能，免除用户反复多次输入繁琐的用户名密码的麻烦，极大的改善了用户体验。同时，降低了因用户重复使用用户名密码导致的帐号泄露概率。

3.3 终端检查与合规检测子系统

3.3.1 PC 终端的安全一体化管理

整体方案要具备终端接入、合规检查、隔离修复、安全防护、审计追溯等“一站式”的入网控制管理流程，适应各单位复杂网络环境下的终端接入控制和实时安全防护、文件审计追溯的要求，保障业务的稳定运行，统一管理要求，从而使终端远程接入的管理变得安全、透明、可控，满足信息安全管理要求。

整体安全防护流程如下：

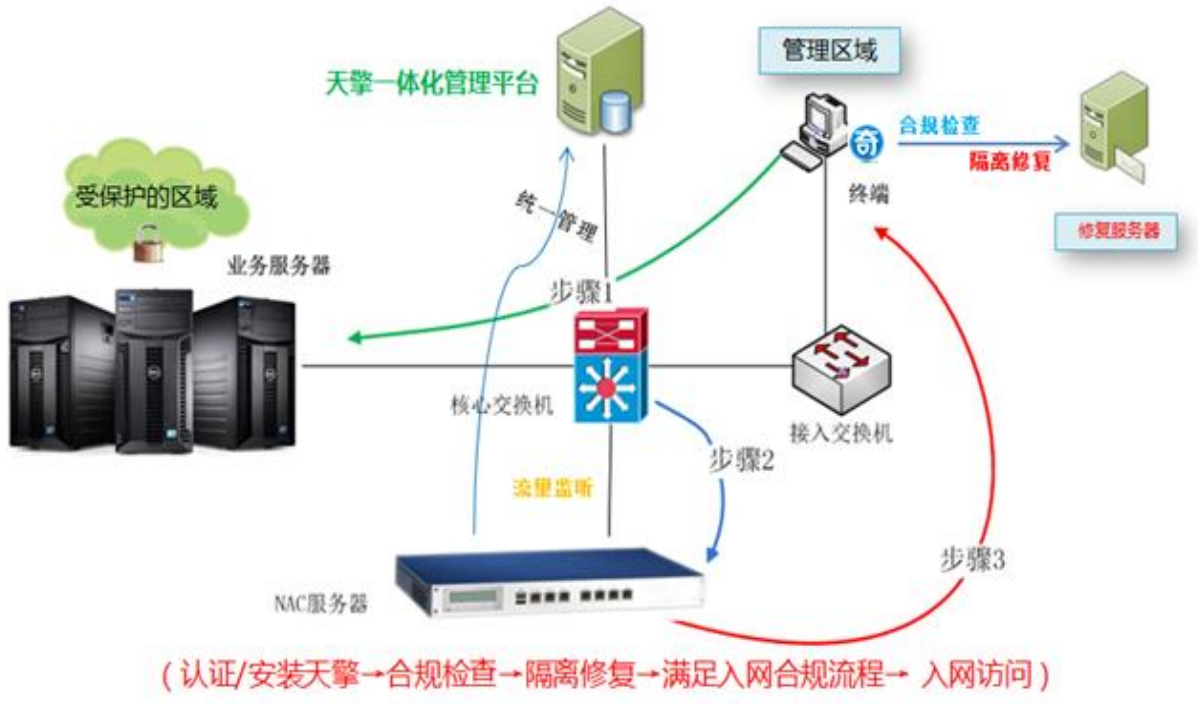


- **终端合规入网：**

可部署旁路 NAC 设备引擎，对于网络结构不产生影响，通过流监听来发现和评估哪些终端入网是否符合遵从条件，可配置入网安全检查策略，不符合进行隔离和修复，达到合规入网的管理规范要求，这种方式的优点在于无需和交换机进行联动，避免交换机管理和配置的复杂性，终端私拉乱接带来的绕过可能性。此轻量级的准入方案，部署简单，上线快，对环境依赖较小，风险和故障点相对较小。

终端的安全防护的一切要素在于安全监测客户端的存在，如果没有安全客户端等于脱离管理，存在重大的安全隐患，终端变成裸奔状态，非可信状态。另一方面是和终端安全软件协同联动，检测入网访问的终端是否安装终端防护点，达到入网遵从条件，可提高客户端的部署效率，防止终端安全软件的卸载和去化率过高，保障入网终端是在安全可控范围内，防止无保护，存在安全隐患的终端访问企业的核心资源，配置合规检查策略也可实现更加细粒度的入网合规要求。

部署架构图如下:

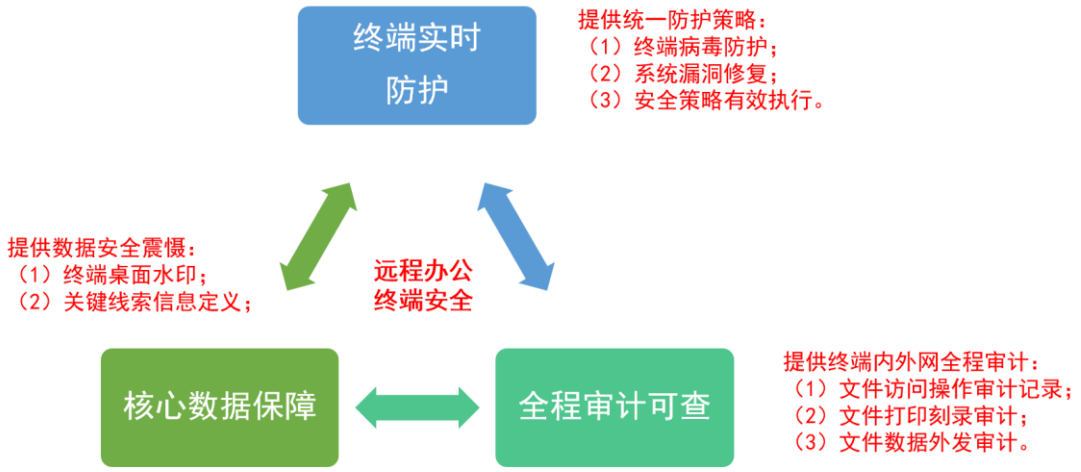


- **终端体检：**

对于接入终端进行安全检查，安全策略会检测终端入网安全状态，能快速定位发现入网计算机终端的安全合规情况，并利用其终端 ACL 防火墙隔离机制立即将这个设备与网络上的其它设备隔离起来，只能够访问自定义的隔离修复区或修复服务器，同时依照策略进行引导式修复或一键修复。对于已确认合规终端，也可调用周期监测或定时监测引擎，对该终端的安全状态进行多次评估，如发现运行阶段又不符合安全检查策略，进行再次隔离或提示，保证入网终端的安全基线是标准的、可控制的，可修复的，并提供一系列入网安全状况统计和终端合规性详情等报告。

安全策略支持多种灵活的处置方式，可只提示不隔离，提示并隔离，手动隔离等多种违规处置手段，适应不同入网强度需求。

实时防护：



实时防护通过一体化平台管理，实现对远程终端安装统一安全防护客户端，具备终端病毒防护、漏洞管理、准入认证、安检合规、管控审计等统一策略配置管理，管理员可以通过控制台直接对网内所有终端进行统一管控。确保全网终端安全看得见、管得住。

终端客户端不受网络环境影响，使用可以根据企业的网络环境自由选择，终端无法连接内网的情况下，也可以选择通过代理或者和互联网环境进行病毒特征库的升级和云查的有效防护。客户端软件本身具备防卸载、防退出能力，保障办公终端的持续安全性。

- **审计记录（核心数据保障、全程审计可查）：**

无论在互联网环境下还是接入到内网环境，终端客户端具备安全审计能力。不仅可以检验合规管理效果，而且是促进内网安全状况持续改善的基本保证。围绕内网合规管理要求，提供了完善的终端行为审计功能，包括：文件操作审计与控制、打印审计与控制、应用程序使用审计、系统开关机审计等多种审计功能。审计内容可以只限定为与内网合规管理相关的信息，保证在达到合规管理审计要求的前提下，充分保护终端用户个人隐私。面向合规的终端行为审计，能够有效确保 100%的终端接受管理监督，促进数据安全状况持续改善。

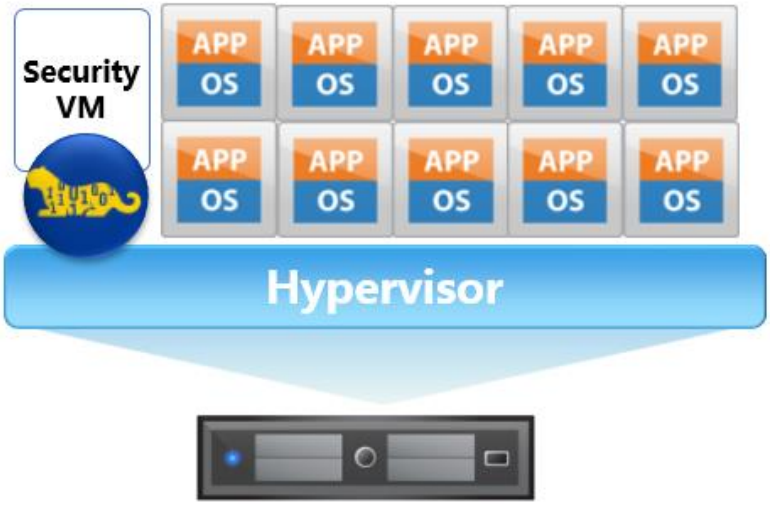
以达到记录终端关键行为日志，帮助管理员进行信息泄漏后的追溯，从终端层面生成记录后结合上层产品，形成整套的安全数据分析方案。

具体审计能力应包含：文件操作审计、文件打印审计、外设使用审计、邮件记录审计。

同时具备屏幕水印能力，可以预防拍照截屏方式泄露业务数据，将终端主机启用屏幕水印功能，屏幕水印会始终保持最前端展示，不管启用何种软件，均可正常显示水印信息。可以通过修改水印文字、显示计算机名、显示用户名、IP 地址、MAC 地址等数据以半透明的方式呈现在屏幕上，屏幕水印功能对拍照等方式泄露数据形成有效的震慑，直接降低了以拍照方式泄露数据的风险。

3.3.2 云桌面无代理防护

以安全虚机（如：VMware、华为）或安全进程（Xenserver、KVM）的无代理方式部署，对所有虚机的恶意代码及时发现和落地查杀，防止恶意代码在网内传播扩散；同时利用主机防火墙实现虚机微隔离，主机 IPS 抵御各类网络攻击，以及利用虚拟补丁等功能来增加虚拟环境下的安全保护。



3.3.3 轻量级 EMM 保障移动终端安全

奇安信 SSL VPN 安全接入网关提供的 VPN 客户端软件，集成轻量级的 MDM 移动安全管理能力，为了保障应用安全、传输数据的安全，同时不改变客户的使用习惯，减少客户的工作量和提升工作效率，奇安信实现了应用封装功能，把业务应用 APP 与 VPN APP 进行封装，解决移动办公场景下用户终端的 APP 数据加密传输及身份认证问题。通过应用商店，管理员可以根据不同的用户和用户组以及对应的权限来推送不同应用 APP 到用户终端上，用户可以在终端上的应用商店列表直接下载安装对应的 APP 进行使用。支持移动终端外设管理，为了保障数据安全性，需要对移动终端的外设进行控制管理，如摄像头，防止在某些环境下造成数据的泄露。支持移动终端密码策略管理，为了保障移动终端安全，防范因

为密码简单而造成的损失，需要对移动终端的密码强度进行管理，加强密码复杂度和难度。

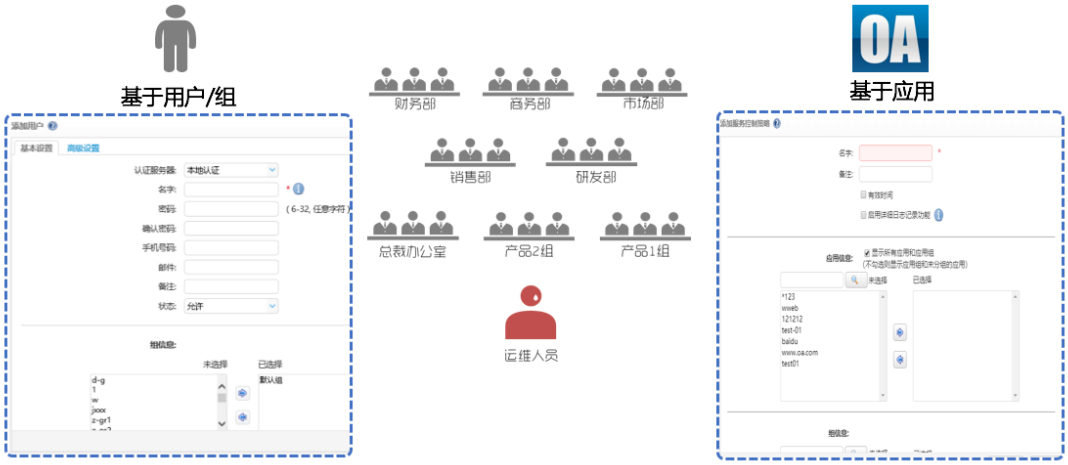
3.4 安全接入及访问控制子系统

3.4.1 链路加密设计

在数据传输过程中，远程用户一旦接入，客户端和服务端通信传输将使用安全的 SSL 加密技术，为客户提供高安全性、高性能、高稳定性的 SSL 接入解决方案，以确保用户账号密码、动态秘钥、应用数据传输的高安全性及稳定性。同时，基于“隧道分离”技术，可通过设置移动终端的隧道控制策略，实现移动终端连接 VPN 后，所有数据只能由 VPN 隧道转发，而不能访问互联网，从而有效规避了移动终端接入企业内网的同时由互联网泄漏关键的业务数据。此外，为了满足国家密码管理相关部门相关规定，进一步加强密码算法的安全性，本方案配置的 SSLVPN 安全接入网关系统完整支持国密算法，包括 SM1、SM2、SM3、SM4。

3.4.2 精细化、细粒度访问控制设计

奇安信 SSL VPN 安全接入网关系统授权机制以多个安全策略维度为中心。用户登录时，会根据用户的属性查询用户的相关安全策略的分配情况，以决定授予用户哪些服务资源，对用户的哪些服务访问采取单点登录策略，对用户的主机绑定策略，以及对用户执行哪些安全策略检查。多维度的授权机制保证了各个安全策略能够独立制定，并分别应用在不同用户。基于 SSL VPN 安全接入网关实现的精细化、细粒度访问控制，能够帮助管理者实现用户级、资源级，甚至精确到 URL 和文件级的用户权限控制。



3.4.3 远程访问行为审计及分析设计

为解决在远程办公和移动办公中的数据安全问题和业务系统运行合规问题，本方案提供了全面的用户行为审计能力和有效的分析能力。可对各类网络设备、安全设备、操作系统、数据库、应用系统的日志、事件、告警信息进行全面的日志采集，日志收集后进行字段和安全等级的归一化处理，收集并归一化后的日志并保留原始日志，方便用户对关键日志快速定位。与此同时，方案提供了实时的日志滚动显示和查询，可自定义实时监视的日志内容，可查看实时日志详细信息，可通过雷达图等直观显示目前日志量，可以控制日志对管理员账号的可见性管理，在实时监视日志上可悬浮提示资产和常用端口信息。

本方案所采用的奇安信日志收集与分析系统，不仅有业界领先的行为分析引擎，也提供了便利的实时分析可视化工具和高效的分析模版。独有的基于安全监测、告警和响应技术（Security Monitor, Alert and Response Technology，简称 SMARTTM）的事件关联分析引擎。在关联规则的驱动下，SMARTTM 事件关联分析引擎能够进行多种方式的事件关联，包括统计关联、时序关联、单事件关联、多事件关联、递归关联，等等。具有领先的事件关联分析核心技术，申请了 4 项专利技术，拥有完全自主知识产权。实时的分析是可视化的，将安全管理和运维人员从繁重的事件查看工作中解脱出来，及时直观地进行事件调查，发现安全威胁。具备强大的事件可视化能力，变用户日常安全管理的认知为感知。通过对用户网络环境中安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统等日志进行全面分析与审计，集成各种合规性关键控制点需求，建立基于日志与行为分析的合规性安全审计平台，为用户提供合规性审计报表报告，充分满足各项标准、法规（萨班斯法案、等保要求、分保要求）的合规性控制需求，降低合规性成本。

3.5 移动办公安全加固子系统

奇安信抗疫远程办公方案的安全移动办公场景，覆盖了移动办公的 6 个环

节，且叠加了业务层的便捷与可信访问能力，全面提升蓝信移动办公的便捷与安全。

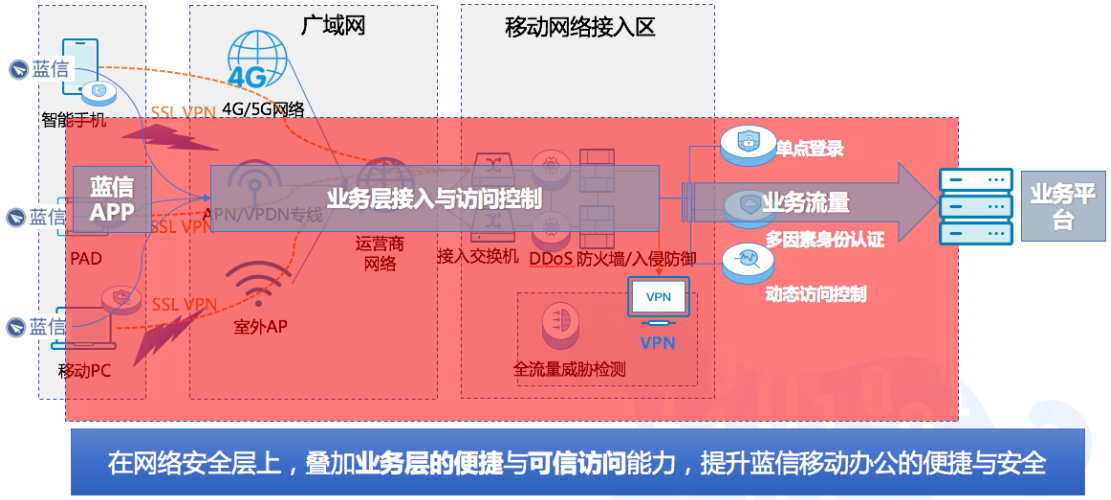
3.5.1 移动终端系统安全

确保移动终端环境的安全可信。内嵌新一代应用沙箱技术，隔离企业应用与个人应用，打造可信的终端环境；

在移动用户认证后，移动用户将在虚拟工作区内处理工作相关的业务数据。同一移动终端设备上既有个人应用,又有企业数据和应用,个人应用可以随意访问、存取企业数据,企业应用同样也会触及到个人数据。为此防止工作区的数据遗落到个人数据区，所以采用虚拟工作区进行数据分离。个人数据与企业数据进行隔离，落地数据加密，第三方应用或转发到其它设备当中无法打开查看。 启用虚拟工作区之后，终端数据落地加密，数据采用 AES256 或者 SM4 加密算法，防止终端数据被拷贝出去而造成数据泄密。当 TrustConnect 被卸载（或 TrustConnect 设备管理器服务被禁用）、设备进行了 Root 或者设备超过一定时间不能连接上网关的情况下，移动终端数据可以远程擦除，防止数据泄密。移动终端隧道控制策略，实现移动终端连接 VPN 以后，移动终端数据只能走 VPN，不能访问互联网，从而实现防止数据泄密。

3.5.2 移动终端链路安全

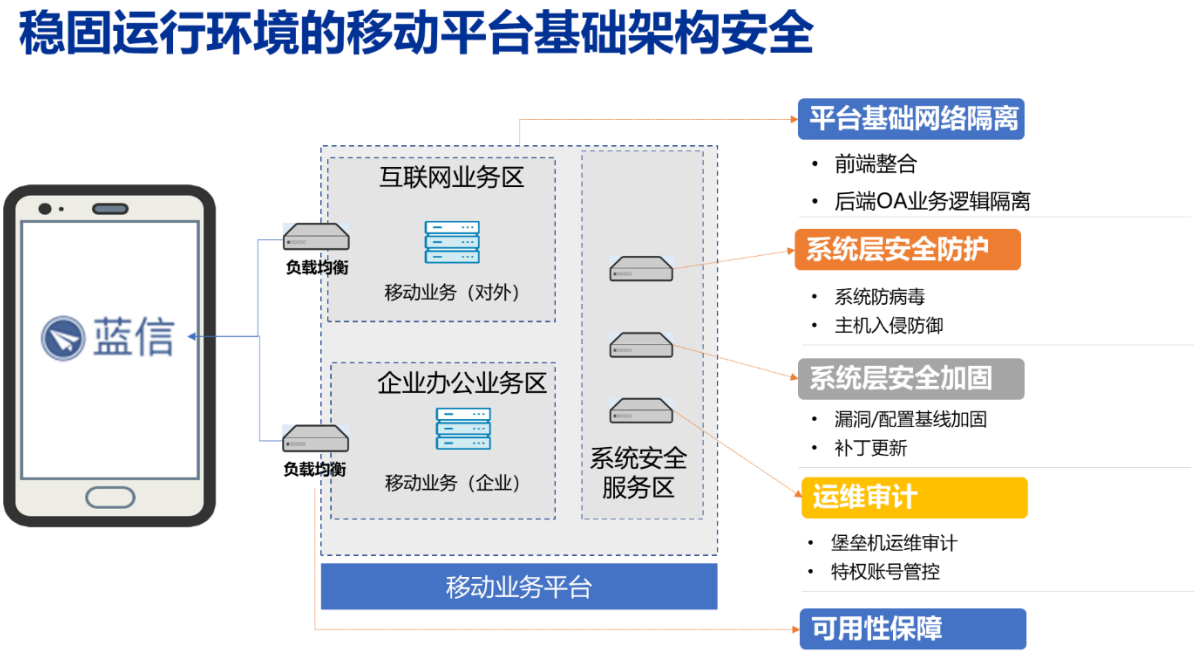
确保移动接入链路的保密可用。在网络安全层上，叠加业务层的便捷与可信访问能力，提升蓝信移动办公的便捷与安全；



在数据传输过程中，远程用户一旦接入，客户端和服务端通信传输将使用安全的 SSL 加密技术，为客户提供高安全性、高性能、高稳定性的 SSL 接入解决方案，以确保用户账号密码、动态秘钥、应用数据传输的高安全性及稳定性。同时，基于“隧道分离”技术，可通过设置移动终端的隧道控制策略，实现移动终端连接 VPN 后，所有数据只能由 VPN 隧道转发，而不能访问互联网，从而有效规避了移动终端接入企业内网的同时由互联网泄漏关键的业务数据。此外，为了满足国家密码管理相关部门相关规定，进一步加强密码算法的安全性，本方案配置的 SSLVPN 安全接入网关系统完整支持国密算法，包括 SM1、SM2、SM3、SM4。

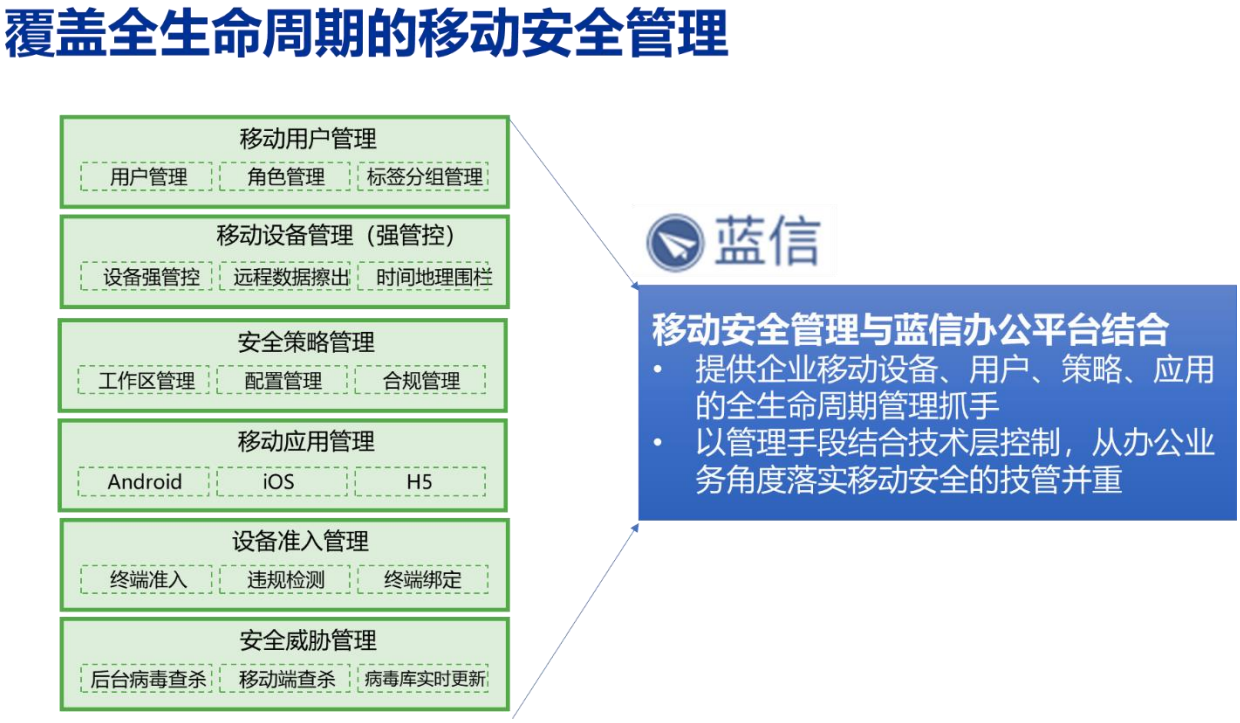
3.5.3 移动终端应用安全

确保移动应用的架构和使用安全。覆盖平台基础网络隔离、系统层安全防护、系统层安全加固、运维审计、可用性保障 5 个方面；



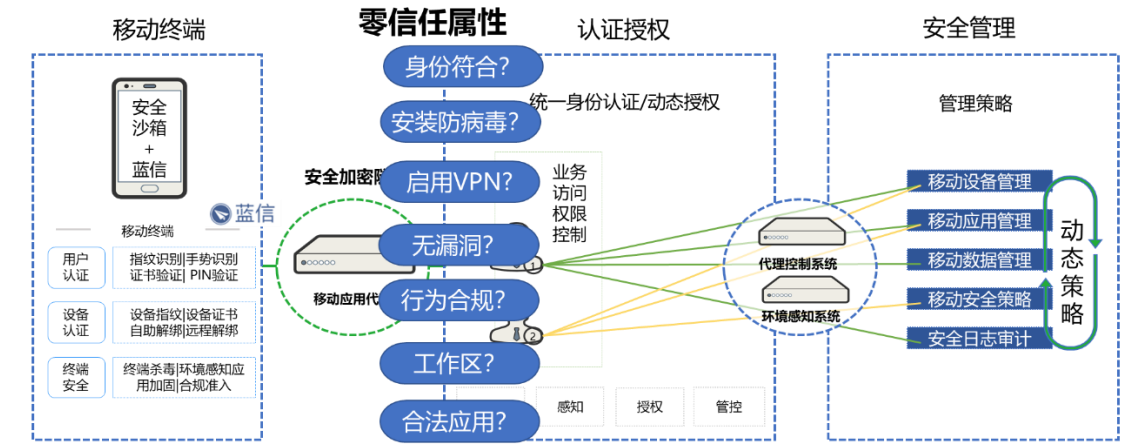
3.5.4 移动终端安全平台

确保移动办公平台的安全运行。移动安全管理与蓝信办公平台结合，覆盖全生命周期的移动安全管理；蓝信提供一个应用统一接入管理平台系统，可将单位内部应用统一接入到蓝信工作平台统一管理，利用蓝信的开放平台、统一数据平台可以对接单位内部现有全部信息化系统，成为各信息系统比如 OA 系统、人力资源系统、BI 系统等的交互枢纽，打破组织内部信息系统之间的壁垒，破除信息孤岛，使协作变得更为高效。同时是蓝信平台基于 RSAP（应用运行自保护）模型开发的移动应用安全管理系统，通过封装（Wrapping）技术将自身多种安全技术注入到应用程序中，与应用程序融为一体，实时监测、阻断攻击，使程序自身拥有自保护的能力。并且应用程序无需在编码时进行任何的修改，只需进行简单的配置即可，以此构建业务 App 内生安全生态环境，保障业务 App 的运行安全和数据安全。



3.5.5 移动终端业务与数据安全

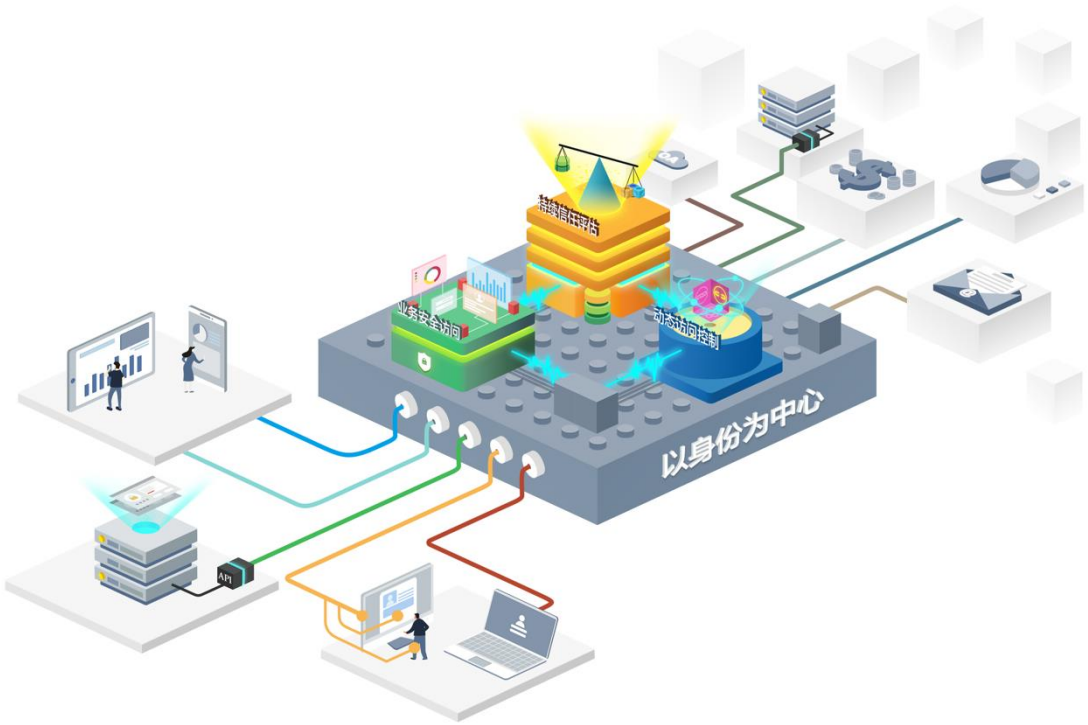
确保移动办公对数据的可信访问及安全流转。基于零信任理念，确保可信的人员使用可信的移动终端，基于可信行为之下访问动态授权的数据，并可基于多种环境属性进行阻断、调整及业务控制；



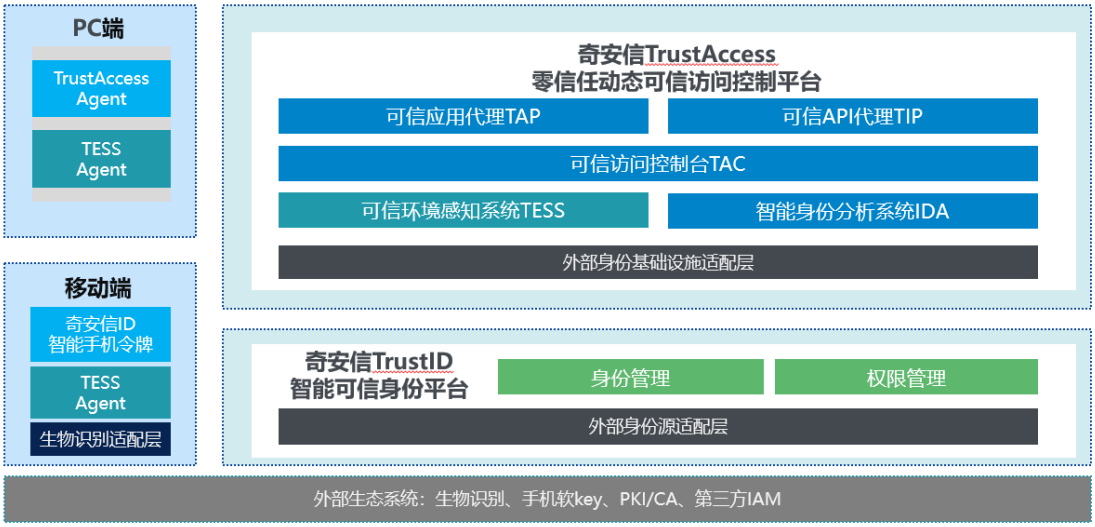
移动办公零信任

在移动办公的复杂场景下，确保可信的人员使用可信的移动终端，基于可信行为之下访问动态授权的数据，并可基于多种环境属性进行阻断、调整及业务控制

奇安信零信任的设计理念，即以身份为中心的动态访问控制，其核心技术要点包括以身份为中心、业务安全访问、持续风险评估和动态访问控制，这些技术要点需要若干技术组件进行支撑，这些技术组件可抽象为可信代理、动态访问控制引擎、身份分析引擎、身份及权限管理，通过这些技术组件，构建动态可信的安全访问平台，作为访问主体和访问客体之间的安全桥梁，保障新 IT 架构下的主体对客体业务、数据访问的安全可信。奇安信零信任身份安全解决方案的核心技术要点包括：以身份为中心、业务安全访问、持续信任评估和动态访问控制，如下图所示：



奇安信零信任身份安全解决方案主要包括：奇安信 TrustAccess 零信任动态可信访问控制平台、奇安信 TrustID 智能可信身份平台和奇安信 ID 智能手机令牌，如下图所示。



依据零信任安全架构的建设思路，进一步设计方案如下：

(1) 梳理核心业务，确定第一优先级的保护目标

大数据中心汇聚了大量高价值数据，因此可直接将大数据中心作为整体保护目标。

(2) 确定高优先级目标的访问路径/暴露面/保护面

大数据中心对外的访问路径包括：用户访问大数据中心的应用、外部应用/应用前置访问大数据中心的服务 API 接口、外部数据平台通过 API 接口和大数据中心进行数据交换。

(3) 梳理各访问路径的主体身份和权限

针对各种访问路径，进一步梳理通过此访问路径对业务和数据发起访问的主体是什么，明确哪些人、设备、应用可能访问此业务和数据。并进一步明确应该赋予各访问主体什么样的访问权限。

(4) 根据安全需求确定访问控制策略

关于环境风险和安全策略，第一阶段首先考虑终端环境的风险，因此，需要将终端环境的风险评估作为访问控制依据。

(5) 分阶段建设访问控制点

针对用户访问大数据中心的应用、外部应用/应用前置访问大数据中心的服务 API 接口、外部数据平台通过 API 接口和大数据中心进行数据交换等场景设计访问控制点，并分阶段建设。

天机以 TrustSpace 的“零信任”安全架构目标是在开放的移动智能终端上构建一个值得信任的企业移动工作空间，为企业级应用与数据提供全面的数据保护方案，从而全面降低由于引入移动智能终端给企业带来的一系列安全风险。TrustSpace 的“零信任”安全是基于设备、人、应用三个维度搭建的一个全新的安全模型，分别如下：

✧ 终端系统环境可信

TrustSpace 通过基于大数据的移动威胁防御（MTD）技术在移动智能终端上提供系统级（如：越狱/Root，系统脆弱性，系统配置合规性检查等）、网络级（如 Wi-Fi 安全检测等）以及应用级（如恶意 APP 行为检测等）的风险感知和威胁检测，确保 TrustSpace 在一个安全可信的移动终端运行环境中运行。

确保移动办公业务的安全合规。可在特定时间、特定地点约束用户使用某些应用、数据传输、外接设备、文档分发、敏感操作等，发现问题可远程关机、重启、擦除、锁定等。

✧ 用户身份边界可信

TrustSpace 通过新一代应用沙箱与身份认证深度技术整合的方式，对企业应用在移动终端上的边界重新进行了划分。这个边界有两层意思，第一层边界是 TrustSpace 自身，它通过应用沙箱技术隔离的方构建了企业应用和个人应用之间的一个基本边界，并且在边界入口处的实施基本身份认证来验证用户的身份。第二层边界的含义是在 TrustSpace 内部会根据应用的不同的价值度和敏感度来定义内部的应用边界，对一些高敏度的应用需要进行基于时间、位置和行为等因素的持续动态的增强身份认证，从而确保这些高敏感或者高价值的应用是在正确的时间和地点被正确的用户安全的访问。

✧ 企业应用数据可信

TrustSpace 通过构建数据全生命周期（存储、传输、使用、共享）保护方案让企业应用/数据变得可信。移动终端数据全生命周期模型，包括数据存储、数据使用、数据共享、数据传输等不同阶段，每个阶段都有一些核心的技术和安全机制来实现数据的保护。在数据存储阶段通过应用层透明加解密技术，在移动终端的存储空间上开辟一个独立的安全存储区域，并对需要落地存储的文件进行高强度加密存储，加密方式可以采用国际 AES 及国密算法两种方式。并且对于数据加密使用的密钥等关键信息通过密钥沙箱技术进行安全存储；在数据传输阶段传输通道上采用基于 T L S 的应用级加密通道，实现在数据传输过程中的安全通道访问；在数据使用阶段需要控制企业员工在使用数据过程中的有意以及无意识的数据泄密行为，比如设置禁止截屏，拷贝粘贴，应用/文档水印等，从而有效的防止企业内部数据的泄露；在数据共享阶段主要限制工作空间内部的应用与应用之间，以及内部应用与个人应用之间的数据共享和交互。


TrustSpace
终端威胁防御
内容审计
移动用户行为分析
蓝信
在蓝信后台对用户使用终端行为监控、终端环境监控、数据内容审核
敏感内容控制
可见性设置
阅后即焚
远程擦除
屏幕锁
水印及文档安全
终端文档水印
文档属性授权
风险用户处置
异常行为检测
用户冻结
离职处置
远程擦除
敏感内容审计
关键敏感词
公告被人审核
应用审核
转出记录审核

4 方案优势

4.1 安全可靠的移动办公平台

1）安全可靠

平台为全国产化开发设计，保证用户拥有数据的使用权和拥有权。，满足各级单位对数据安全的要求。

2）移动统一入口，兼顾平战需求

考虑对于应急场景（“战时”）和移动工作场景（“平时”）的多样性复杂需求的实际，疫情期间可进行应急处置，疫情结束仍可作为办公平台实现在线办公，后续可以地方其他项目进行无缝衔接。

3）组织流程处置移动化

充分解决组织内部、相关机构和部门“连不上、听不到、看不见” 的痛点，实现中央、各级组织、单位、各疫区统一指挥安排，提高跨组织协调效率；

4）数据报送全流程电子化和规范化

解决中央、疫情一线基层单位信息经上报层层传递，信息传递滞后问题，及时通报疫情和灾害情况，客观收集信息，统一信息来源。

5）实时监测，信息透明

充分发挥移动终端的便捷与通报及时等特点，远程视频调度指挥，直连一线，便于各级单位和部门快速透明进行信息通报处置。

6）超大群组沟通，满足多组织沟通需要

蓝信支持 2000 人以上超大群组，并可对组织通讯录分级分权控制，兼顾沟通顺畅和个人信息安全。实现跨组织、跨部门的沟通办公需要。

7）一键 500 方电话会议，会议指示即时下达

最高可支持 500 人同时发起电话会议。电话语音，不受网络质量影响，移动端和电脑端同步管理会议，参会人可以通过会议群共享文件。支持群组内成员，全部/部分成员批量快速入会。

8）自身情况每日报告，自身健康监测

针对疫情期间，个人可通过移动端每日上报自身情况，方便领导及时获取内部员工信息。

4.2 网络架构无影响、终端防护无感知

在网络核心交换从旁路部署 NAC，对于网络架构无影响和冲突，同时对于接入到内网未安装终端安全管理软件的计算机进行安装指引，并提供病毒查杀、安全检查、补丁修复、全程审计的主要功能，将功能集中在一客户端中，保障用户

使用的高效和稳定性。

4.3 终端接入即合规、全面体检看风险

基于统一安全策略进行要求，无论公司派发终端、私人终端接入内网必须按照单位统一安全防护进行要求，接入终端必须满足安全防护能力，并进行 20 余项安全体检，发现潜在感染源进行隔离处置，保障内网安全性。

4.4 行为全程在审计、桌面水印强震慑

对于在家办公期间，对于单位核心文件的操作、打印、外发等动作全程记录，并通过内网环境进行上传，待在发现异常事件后，管理人员可做到有据可循，快速定位违规事件，同时通过屏幕水印能力，让远程办公人员对于核心文件的规范化处理做到认真对待。

4.5 个人数据与工作数据安全分离

移动终端采用移动沙箱技术设计双区域模式：工作区模式和个人区模式。工作区数据应用和个人区数据应用完全隔离。工作区内的数据无论是存储还是通讯都经过加密处理，并且企业管理员具有对设备数据的删除权限，很好的保护企业数据不被泄漏。

4.6 业界独创软 Token，便捷启用多因素认证

奇安信 ID 身份认证系统独创 SecToken 技术（软 Token）。SecToken 以软件 app 形式部署在智能移动终端中，并通过模块化的 License 控制植入在硬件 VPN 中。可以为客户节约购买硬件 Token、Token 认证服务器的硬件成本。

5 解决方案产品清单

解决方案	产品	主要功能	形态与部署
安全远程接入办公	SSL VPN 安全接入网关	提供专用加密隧道，保证通讯传输安全，并执行细粒度、精细化访问控制，终端安全审查	硬件，旁路部署于企业网络外联区
	奇安信 ID	提供基于生物识别及设备指纹的动态验证口令，实现多因素认证	客户端：软件，安装于远程接入用户手机 管理端：硬件，部署于企业网络运维区

	天擎	统一防护策略：终端病毒防护、系统漏洞修复、安全策略有效执行； 数据安全震慑：终端文件水印、外发监测； 内外网全程审计：文件访问操作审计记录、文件打印刻录审计、文件数据外发审计。	客户端：软件，天擎客户端 控制中心：软件，对于客户端和准入进行策略配置。 NAC:硬件，部署于企业网核心交换处。
	日志审计与行为分析	日志收集、行为分析、网络安全状态分析等	管理端：软件，部署于企业网络运维区，需收集 SSL VPN、认证、终端防护等相关日志
	虚拟化安全管理系统	为虚拟桌面提供无代理的防病毒、防火墙、IPS、应用管控的功能	客户端：软件，以安全虚拟机(vmware)或部署于 Xenserver、KVM 虚拟化层中； 管理端：软件，部署于企业网络运维区
	天机	杀毒、数据防泄漏、水印、MTP 移动威胁防御、强广管控、SSL VPN、应用套件、可信应用商店、新一代应用沙箱等	移动端：软件，安装于远程接入手机 管理端：软件，部署于企业网络运维区
	蓝信	即时通讯、电话会议、视频会议、考勤、邮件、OA、行政审批、工作日志等	客户端：软件，安装于远程接入手机 管理端：软件，部署于企业网络运维区；或使用 SaaS 服务